

CSO

What Kind of Target Are YOU?

Find out how to protect what makes
you worth attacking

28



TECH: Mobile Boom Has Spawned
Global Criminal Marketplace **6**

RISK: Forget Being CSO—
Companies Need CROs **16**

LEAD: What Makes an Awareness
Program Work **22**

SPLUNK AND YOU SHALL FIND.

The threats you know about. And the ones you don't.

Finding advanced threats requires a different approach. Splunk® software lets you collect and visualize your machine data and apply statistical analysis to it in real time. Move beyond the scalability limitations of traditional security tools to detect both known and unknown threats wherever they might appear. Discover the world's fastest growing real-time platform for security intelligence and defend against today's most sophisticated and malicious attackers.

Learn more at splunk.com/goto/security

splunk > listen to your data™

© 2013 Splunk Inc. All rights reserved.



COVER STORY

What Kind of Target Are You?

28 Some attackers want money or data, while others hope to make you look bad. What do you have that might put you on a hacker's hit list?

BY BOB VIOLINO

■ Also Inside

2 Editor's Letter

4 Publisher's Letter

32 Last: Ten Tweets with David Litchfield

September 2013 Volume 12, Number 7



6

tech

6 Mobile Boom Has Spawned Global Criminal Marketplace

7 Google Play Store Suffers Deluge of Scam Apps

8 OpenDNS Foresees Attacks Before They Happen

10 Are Smartphones Killing Passwords?

12 Hackers Use Compromised Business Domains to Host Images of Extreme Child Abuse

14 On the Lookout for Email Scams? They're Not What You Think

15 Car Hack Highlights March Toward Remote Control of Critical Systems



14



16

risk

16 Forget Being CSO—Companies Need CROs

17 Rise in Data Breaches Drives Interest in Cyber Insurance

18 3 Things to Consider Before Buying Into Disaster Recovery as a Service

20 Workers Expose Data in Quest for Productivity



20



22

lead

22 What Makes an Awareness Program Work

24 Beef Up Defenses Without Breaking the Bank

26 Using IT Skills to Help the World's Poorest



26

Rethinking Your Value to a Criminal

There's a theme that ties together many of my conversations with security folks: Everyone has something that's valuable to a criminal.

What frustrates many of the people in the business of protecting organizations' critical assets is that this message is a hard one to sell to others. Unfortunately, there are still many businesses out there, particularly the small and midsize organizations working with a minimal security budget, who prefer to think they don't have anything a hacker would want.

As this month's cover story points out, that's a dangerous assumption to make.

The bad guys are coming after data, money or even your good name. Last month alone, we saw multiple hits on major media outlets by the Syrian Electronic Army, a group of hackers who support Syrian President Bashar al-Assad. The attackers managed to break into the website of *The Washington Post* and redirect readers to their own Web page, and the same group compromised several accounts belonging to the *New York Post*, including the publication's Twitter feed.

In this month's issue of *CSO*, we break down why certain companies prove to be popular targets for hackers. Sometimes it's the type of services they offer, or the number of outlets



that comprise an organization, that places a company directly in the crosshairs of an industrious thief.

We hope after reading you'll have a better idea of just what you've got that a criminal may want access to, and, more importantly, how to take the proper steps to protect what's precious to your organization.

—Joan Goodchild, editor
jgoodchild@cxo.com

CSO

Editor

Joan Goodchild
jgoodchild@cxo.com
508 988-7994
Twitter: @msjoanieg

Senior Editor, Copy and Production

Colleen Barry

Art Director

Steve Traynor

Staff Writer

Steve Ragan
sragan@cxo.com
Twitter: @SteveD3

Editorial Administrator

Pat Josefek

Research Manager

Carolyn Johnson

Contributors

Taylor Armerding, David Geer,
Antone Gonsalves, George V. Hulme,
Jeremy Kirk, John P. Mello Jr.,
Lauren Gibbons Paul, Bob Violino

Editorial/Advertising/

Business Offices

492 Old Connecticut Path,
P.O. Box 9208
Framingham, MA 01701-9208
Main phone number: 508 872-0080

Subscriber Services

Phone: 866 354-1125
Fax: 847 564-9453
cs@omeda.com

IDG Enterprise
An IDG Communications Company

International Data Group

Chairman of the Board

Patrick J. McGovern

IDG Communications, Inc.

CEO

Bob Carrigan

Chief Content Officer

John Gallant

BPA
WORLDWIDE™

CSO (ISSN 1540-904X) is published monthly except for a combined issue in July/August and December/January by CXO Media Inc., 492 Old Connecticut Path, P.O. Box 9208, Framingham, MA 01701-9208. Periodical Postage Rate at Framingham, MA 01701, and at additional mailing offices. Canadian Publications Mail agreement number 1902075. Canadian Postmaster: Please return undeliverable copy to P.O. Box 1632, Windsor, ON N9A 7C9. Copyright 2011 by CXO Media Inc. All rights reserved. Reproduction of material appearing in CSO is forbidden without written permission. Permission to photocopy for internal or personal use or the internal or personal use of specific clients is granted by CSO for users through the Copyright Clearance Center, provided that a fee of \$3.50 per copy of the article is paid directly to Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01970. www.copyright.com. Please specify: ISSN 1540-904X. Permission to photocopy does not extend to contributed articles—followed by this symbol: †. Address inquiries to CSO, P.O. Box 3482, Northbrook, IL 60065; 866 354-1125. CSO is free to qualified security executives. To all others the one-year basic rate is \$70 for the United States and Canada, \$95 to foreign countries (payable in U.S. funds only). The single copy price is \$9 to the U.S. and Canada and \$15 International. Please allow four to six weeks for new subscriptions to begin. Change of Address: Go to www.ameda.com/custsrv/cso and follow the online instructions. Postmaster: Send change of address to: CSO, P.O. Box 3482, Northbrook, IL 60065. Printed in the USA.

Avigilon spotted a man in this



who was caught



and identified by his



Meanwhile, analog identified



Only our high-definition surveillance solutions give you the full story. Identify incidents quickly and enhance response times with the superior image detail of an Avigilon end-to-end system. See how Avigilon can help your organization at avigilon.com/casestudies

The top three images were shot with an Avigilon 29 MP HD Pro camera. The fourth image was shot with an analog camera.

avigilon
THE BEST EVIDENCE™

Who Handles Enterprise Risk Management?

As security leaders, do you feel like people are always trying to credit others with the work that you do and the things you are responsible for? You must, because every time I turn around, some vendor or analyst or someone is telling me that others in your organization are responsible for what you do.

Identity management? That's some network admin. Mobile security? That's the CIO. Enterprise risk management? Well that's a bunch of people including the CIO, the CFO, the COO and the chief risk officer, but not including you and the board of directors.

This seems to be an ongoing problem, but for these people to ignore the larger responsibility of enterprise risk management is really a disservice to you. You have been leaders in enterprise risk since before it was called enterprise risk. We once referred to it just as operational risk. Some organizations still split risk into IT risk, operational risk and capital risk. But as leaders in providing a holistic view of risk to the business, you have often been the people who have dragged your organizations along kicking and screaming. That has become a bit easier recently as boards of directors have a newfound interest in enterprise risk and the benefit of looking at things in an integrated, holistic manner.

So why are many of you still underappreciated by others who try to define the landscape of enterprise risk responsibility?

It's probably not malicious. I honestly believe that a lot of it has to do with the fact that these folks just don't understand the way that thinking about business risk is evolving. They still function in the IT-centric and finance-centric



worlds of the past, and those worlds handle risk very differently than the way many of us believe it should be viewed and managed today.

Embrace your special place in enterprise risk management because it represents the important contribution that you bring to your organization.

And make sure you are yelling about it from the rooftops. As always, the only person that will advocate for you is you.

—Bob Bragdon, publisher
bbragdon@cxo.com

Advertiser Index

Avigilon	3	HID Corp.	9	Tyco Integrated Securities.	5
BMC Software	C4	Milestone Systems Inc.	11	Vormetric, Inc.	C3
CSO	21, 27	Splunk	C2	Websense Inc.	13

CSO

Executive Committee

President & CEO Michael Friedenberg

Executive Assistant to the
President & CEO Pamela Carlson

SVP of Human Resources
Patricia Chisholm

SVP of Events Ellen Daly

SVP & Chief Content
Officer John Gallant

SVP of Digital Brian Glynn

SVP of Strategic Programs &
Custom Solutions Group Charles Lee

SVP, Group Publisher & CMO Bob Melk

SVP & General Manager,
Online Operations Gregg Pinsky

SVP of DEMO Neil Silverman

SVP & COO Matthew Smith

SVP & General Manager,
CIO Executive Council Pam Stenson

SVP of Digital, &
Publisher Sean Weglage

Sales

Publisher Bob Bragdon

East Coast Regional Director,
Integrated Sales Roz Burke

Sales Director – West Mary Hazelton

Sales Assistant Kelsey Scheldemantel

Integrated Media and Online Sales

East Coast Online Regional Sales
Manager Richard Hartman

West Coast Online Regional
Sales Manager Erika Karr

Central Online Regional Sales
Manager Carmen Facas

Director of Ad Operations &
Project Management Bill Rigby

Director, Online Account
Services Danielle Thorne

Production

VP Production Services Chris Cuoco

Production Manager Heidi Broadley

Marketing

Vice President, Marketing Sue Yanovitch

Marketing & PR Manager Lynn Holmlund

List Services

Contact Steve Tozeski of IDG List Services
at 508 820-8106 or stozeski@idglist.com

Reprints & Permissions

For information about reprints and
copyright permissions, please contact
The YGS Group, 800-290-5460, ext. 100,
cso@theygsgroup.com

What would a quarterback know about defense?

Stop by and **ask him.**



Steve Young / Football Legend
Meet him at ASIS.



Over the course of a 14-year career, Steve Young learned a thing or two about keeping his team moving in the right direction – and staying one step ahead of the bad guys. That last year's clever innovation is probably already out of date – and that the best defense is a smart offense. We like Steve Young – and we think you will too. He thinks like we think.

80 percent of the world's Top 100 retailers, 9 of the Top 10 banking institutions, 2/3 of the nation's busiest airports, and every U.S. Federal Courthouse entrusts the safety of their enterprise to Tyco Integrated Security. Because we never stop thinking about how to help them improve their business security, safeguard their properties, and save lives. It's our passion – and the reason why we're the world's leading security integrator. Let's explore how we can help you.

Safer. Smarter. Tyco.™ | 1.800.2.TYCO.IS

Visit us at **ASIS 2013 - Booth 805**/ Get your free Expo Pass at www.tycois.com/ASIS2013

License information available at www.tycois.com.

©2013 Tyco. All rights reserved. Tyco is a registered trademark. Unauthorized use is strictly prohibited.

tyco
Integrated Security

tech

TOOLS SYSTEMS NETWORKS DATA PRIVACY



Mobile Boom Has Spawned Global Criminal Marketplace

Report reveals that criminal infrastructure targeting mobile has sprung up much faster than it did for PCs BY JOHN P. MELLO JR.

MOBILE DEVICES HAVE BECOME ENTICING targets for criminals around the world, so much so that an underground industry has begun to grow to support malicious activity aimed at those devices, according to a report by the Anti-Phishing Working Group (APWG).

"In a 'post-PC era,' mobile devices increas-

ingly present an attractive, practical and economical alternative to traditional desktops," said the report, titled "Mobile Threats and the Underground Marketplace."

"In the coming years," it continued, "global mobile payments are predicted to exceed \$1.3 trillion, moreover, presenting a mother lode of opportunity for cyber crime gangs who appreciate the vulnerabilities of these peripatetic communications and computing platforms."

The purpose of the report is to provide a comprehensive look at the criminal infrastruc-

ture growing around mobile fraud, says APWG Chairman Dave Jevans, who is also chairman and CTO of Marble Security. "When you look how that underground economy works, you can see a big infrastructure being built for mobile electronic crime," he says.

That infrastructure is being created much faster than it was for PC fraud. "It's growing at least five times faster," Jevans says. "What took 10 years for PCs is going to take 18 months to two years for mobile."

Some of the mobile crime infrastructure is

being built on the existing components of the PC crime network. For example, "bulletproof" hosts used to host phishing sites and malware distribution are now used for hosting Android malware, mobile toolkits and SMS phishing.

"A large part of the infrastructure providers for electronic crime over the last 10 years are merely adding mobile into their mix, so everything is moving much more quickly," Jevans says.

This has been a natural progression for the underground digital-weapons bazaar, says Tom Kellermann, vice president of cybersecurity for Trend Micro. He says the trend in mobile crimeware began six or seven years ago when the Asian and European banks decided to push mobile banking initiatives.

"You began to see traditional crime kits like Zeus, SpyEye and Citadel add mobile variants," he says.

Mobile devices can be more vulnerable to man-in-the-browser attacks because both their regular Web browsers and their apps interact directly with the Web.

"The browsers in the mobile devices become the Achilles heel because they're providing the session for the authentication to occur, which is why there are so many successful man-in-the-browser attacks that are focused on mobile platforms," Kellermann says.

Another aspect of many mobile devices that makes them easy targets for cybercriminals is their small screens. "That means you don't see the hints and the clues you'd get with a desktop or laptop that something is wrong with what you're looking at," says Tim Chiu, director of product marketing for security at Blue Coat Systems.

For example, in a phishing attack on a desktop, there are clues that tell you it's an attack—you can see the full URL of where you're at or hover over a link to see where it goes. "On a mobile device, you can't hover, so you never know the actual URL you're going to when you tap it," Chiu says.

"And when you go to a URL," he continued, "many mobile devices have a feature called 'auto hide' in order to give you the most real estate on your little screen as possible. That hides the URL so you don't know where you are."

Despite the attention mobile devices are grabbing from cybercriminals, it may take a watershed event to bring the point home to the public. "We'll have a big problem when the first widespread Apple malware occurs that is financially targeted," says Ken Baylor, a research vice president for NSS Labs.

"While Apple has the ability to yank bad applications once they're installed, as we saw in the recent \$45 million ATM fraud scam, the things you can do in eight to 12 hours are pretty amazing," he says.

■ John P. Mello Jr. is a freelance writer and regular contributor to CSO.



Google Play Store Suffers Deluge of Scam Apps

A STEADY STREAM OF QUESTIONABLE APPS IS flowing daily into Google's Play store for Android devices, according to security vendor Symantec.

Over the past seven months, Symantec found more than 1,200 suspicious apps in the Play store. Google removes many shortly after they're published, but others stay in the store for a few days.

"Although they have short lives, the apps must provide ample profit for the scammers as they show no signs of halting their development of new ones," wrote Joji Hamada of Symantec.

The applications can be difficult to assess and employ a series of maneuvers and layers to rip off users.

Hamada wrote that one application aims to get users to subscribe to an online adult video site at a cost of more than \$3,000 a year. The app launches a link to the site, which then asks the user to register to play videos. An email form is drafted, and the user is asked to hit send. The email, sent to the user, contains a link to another service on a different website.

This time, the user is prompted to enter a password. If that button is clicked, the phone is supplied with a number that, when called, gives out a password. The user is given registration details and then told that there is a \$3,200 annual fee that is due within three days.

Applications that only launch links "can be almost impossible for any system to confirm anything malicious," Hamada wrote. "The manual steps required in this scam is another strategy used to keep the apps on the market as long as possible. Human analysis may be the only way to discover these sorts of apps."

More than 100 applications similar to the adult videos one were published on Google Play in July alone, Hamada wrote. Symantec informs Google when it finds such applications, he wrote, but the scam applications flow into Play daily. Many of the apps float into some of the top keyword searches, apparently thanks to abuse of Play's search function.

—Jeremy Kirk



SALTED HASH

OpenDNS Foresees Attacks Before They Happen

I'M FAMILIAR WITH OPENDNS, OR AT least I thought I was.

I've used the service before when I just needed a reliable DNS server to connect to. But it had never crossed my mind that OpenDNS might be considered a security company, so I was surprised to run into representatives from the company at a Black Hat reception hosted by Cylance.

It turns out—to OpenDNS' credit—that the leadership of the company didn't fall into the same trap I did. Rather than assuming the company provides DNS services and viewing the world strictly through that limited lens, OpenDNS stepped back and considered the bigger picture.

The fact is that by virtue of providing DNS services, OpenDNS has an inside view of massive amounts of Web traffic, and that data has security value.

OpenDNS had unveiled its Umbrella Security Graph, a big-data-mining outlet of the company, at the Kaspersky Threatpost Security Analyst Summit earlier this year, although the Black Hat reception was the first time I'd heard of it. CTO Dan Hubbard used the occasion to demonstrate Umbrella Security Graph's ability to discover attributes, domains and locations connected with the Red October cyberespionage attacks.

Applying big data algorithms to analyze traffic in real-time, OpenDNS can predict which IP addresses or domains will be malicious before there's even an attack to detect.

In a press release from the Kaspersky event, Hubbard is quoted as saying, "The mission of the Umbrella Security Labs is to continually innovate ahead of the pace of technology change and build the best security protection and security delivery network platform possible without compromising performance or productivity. By partnering with other entities that can contribute additional data scoring techniques, data mining capabilities and visu-

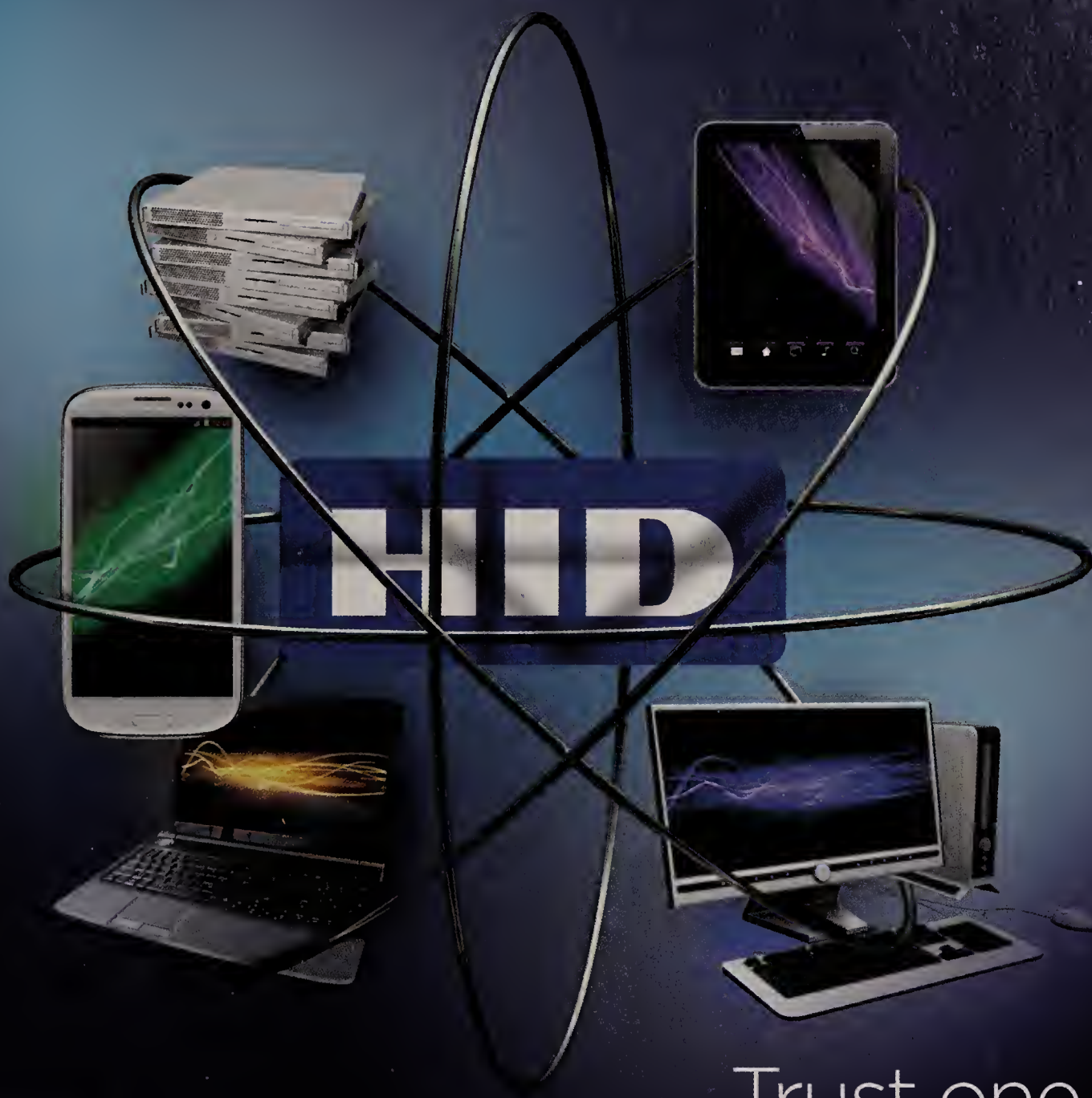


al graphs we can transform from the Internet security industry from reactive to predictive."

That's a tall order with a lot of buzzwords, but the concept sounds intriguing. I did not get a chance to view the demo myself yet, but

I hope to attend an upcoming OpenDNS event and learn more about the how the company is leveraging the vast quantities of data it has access to in an effort to make the Internet a safer place for its customers.

T H E P O W E R O F O N E .



Trust one.
Identify all.

Learn about the assurance that comes with the Power of One. hidglobal.com/powerOne or Scan this with a QR reader



Only HID Global has the capability to take care of all your company's identity assurance needs through a single trusted source.



From IT to corporate security, from credentials to authentication to management services, HID Global is the only one ready to provide a best in class Identity Assurance solution that goes beyond a simple password. Each user receives a single identity credential that can be authenticated across multiple access points and devices. One identity. One security policy. One trusted source. Only from HID Global. The Power of One.

For more information, visit hidglobal.com/powerone-cso

© 2012 HID Global Corporation/ASSA ABLOY AB. All rights reserved. HID, HID Global, the HID Blue Brick logo and the Chain Design are trademarks or registered trademarks of HID Global or its licensor(s)/supplier(s) in the US and other countries and may not be used without permission. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.

Are Smartphones Killing Passwords?

THE UBIQUITOUS SMARTPHONE, which many people now depend on for business and in their personal lives, is emerging as a promising replacement for passwords used in authentication.

Most experts agree that we have to do away with passwords to bolster website security. The effectiveness of passwords is severely undermined by people's fondness for easy-to-guess, often-reused codes. In addition, sophisticated decryption technology has made even encrypted passwords easily acquirable by hackers.

Because a smartphone is the one device few people are ever without, it may be the perfect place to store credentials. Also, the devices include many sensors that can identify a user.

"I think it's brilliant," says Trent Henry, analyst for Gartner. "We're finding that [smartphones] will be the type of authentication mode in the future."

A number of vendors, including Authy, Clef and Duo Security, are trying their best to drive the industry in that direction. Even large security companies are getting into the market. Last month, EMC-owned RSA acquired PassBan, which provides technology that turns smartphones into voice- and facial-recognition machines that can be used for multifactor authentication.

Today, most vendors use smartphones for two-factor authentication. When a person logs in to a website, a unique PIN is sent to their phone. Inputting the PIN completes the sign-in process.

Unfortunately, most consumers are unwilling to take those extra steps, so the search for an easier and more seamless method continues.

Authy moved in that direction last week with the introduction of an app that connects an iPhone or Android phone to an Apple computer via Bluetooth. From then on, when a person visits Facebook, Dropbox, Gmail or another supporting website,



the credential stored in the phone is used to log in to the site automatically.

Authy founder and CEO Daniel Palacio sees the app as only a beginning. In time, the same authentication tools could be run through Google Glass, a digital watch or some other type of wearable computer.

Authy's work and that of its competitors reflect the industry's search for the perfect solution, which is still a ways off.

"The frothy experimentation in the market means we haven't found the right sweet-spot solution yet, and we may never find a single one that suffices for all scenarios," says Eve Maler, analyst for Forrester Research. "Passwords are unlikely to be entirely supplanted unless that single solution appears someday."

For mobile phones to replace passwords, the devices will have to know when the actual owner is logging in to a site, as opposed to someone else that stole or found the phone. Biometrics is one possible answer, assuming reliable and highly secure

fingerprint scanners and voice and facial recognition technology can be developed.

Another possibility is phone sensors that can identify the user by the way he or she walks. The Georgia Institute of Technology and MIT are currently experimenting with this kind of technology, called gait recognition.

Once biometrics becomes a rock solid way to identify a device's user, "we'll start to have a very, very, very secure authentication system that's very hassle-free," Palacio says. "People just buy it and it works."

While such a system may be much better than the passwords now in use, it does not mean hackers will be out of business.

"The attackers continue to go after these new techniques, so we have to be very careful about the security properties," Henry says.

"In other words, you still have to evaluate what kind of attacks could occur."

—Antone Gonsalves



Conservation. Protecting the wildlife of South Africa's Kruger National Park from poachers was once an impossible challenge. But today the park uses Milestone XProtect® Enterprise and integrates license plate recognition to track poachers' vehicles from one central location. Proving again that Milestone can solve problems that are more than security.

More than security

Milestone XProtect® is the world's leading IP video surveillance management software and is reliable, future proof and easy to use. It supports the widest choice in cameras and seamlessly integrates with business and security solutions such as license plate recognition. Which means your possibilities are unlimited and you can keep your security options *open*.

Discover the Power of Choice and the new ways to use XProtect at: www.milestonesys.com

Milestone Systems U.S.
Tel: 503 350 1100



The Open Platform Company

Hackers Use Compromised Business Domains to Host Images of Extreme Child Abuse

THE INTERNET WATCH FOUNDATION (IWF) says compromised websites, owned by legitimate businesses, are being used to deliver some of the worst images of child sexual abuse seen in some time.

The IWF, a U.K. nonprofit funded by Google, Virgin Media and British Telecom, has been working since the mid-1990s to take down illegal content online, includ-

seeing some of the worst images of child sexual abuse," the IWF said in a statement.

In an effort to remain undetected, the images are not available to the public directly. Rather, they are accessed from other websites that deliver adult content. So while a user is visiting an adult website rendering legal content, once an image or video is accessed, a script will redirect them

lated to young people or children.... Since identifying this trend, we've been tracking it and feeding into police forces and our sister hotlines abroad," says IWF Technical Researcher Sarah Smith.

While there will be no legal repercussions for those who reported their discovery, they will probably suffer mental and emotional distress for quite some time.

The images, the IWF explained, show infants and children up to 2 years of age.

Current speculation says that the hijacked business domains and the horrific images are part of an effort to bypass content filtering in the U.K., which will restrict access to pornographic content related to rape and child pornography.

"One of the oldest methods for covert Web publishing is to set up a website on a suitably boring anodyne topic...but have the main covert material only accessible via an un-indexed absolute URL," digital forensics expert Peter Sommer told *Wired* U.K.

"The disadvantage is that you will still be traceable via your contract with the ISP supplying you with web space and your Whois data. But if you can find someone else's poorly secured Web server, you can pull off the same trick."

According to the IWF, there were more than 9,477 websites hosting images of abuse on the Web in 2012, but those are only the sites that were reported.

"What is concerning for us is that not enough people know how to report this or would rather ignore it," says IWF CEO Susie Hargreaves.

—Steve Ragan



ing child pornography. Over the past six weeks, the organization says it has received 227 complaints from people who accidentally discovered this content, much to their shock and horror.

Based on research conducted by the IWF, one example included a furniture store that had its domain compromised. After gaining access, the attackers uploaded to the website a folder containing hundreds of child sexual abuse images, showing very young children and severe levels of abuse.

"This technique of hacking websites also means online surfers are being tricked into

to the abuse images hosted externally on the compromised domain.

In each stage of this attack, neither the legitimate adult-content provider nor the compromised business have a clue what's happening.

"We hadn't seen significant numbers of hacked websites for around two years, and then suddenly in June we started seeing this happening more and more. It shows how someone, not looking for child sexual abuse images, can stumble across it. The original adult content the Internet user is viewing is far removed from anything re-

WHO'S GOT THEIR HANDS ON YOUR DATA?

WANT TO SEE HOW YOUR DEFENSES ARE BYPASSED?

TRADITIONAL SECURITY NO LONGER SECURES.

There's a town in Romania known as Hackerville. It's where criminals turn data into expensive sports cars. This isn't just credit card fraud, this is monetizing intellectual property swiped from companies who thought they were protected.

We know where the bad guys lurk. Not just in Hackerville, but also in your network's blind spots. Put us to the test.

TRITON STOPS MORE THREATS. WE CAN PROVE IT.

www.websense.com/proveit

websense



websense
TRITON

© 2013 Websense, Inc. All rights reserved. Websense and the Websense logo are registered trademarks of Websense, Inc. in the United States and various countries. All other trademarks are the property of their respective owner.

On the Lookout for Email Scams? They're Not What You Think

EMAIL FROM SOCIAL MEDIA BRANDS IS SOME OF THE safest on the Internet, while electronic posts from financial services brands is some of the riskiest, according to a report from Agari, an email security provider.

"Consumers may be worried about their privacy settings, but in terms of protecting consumers via email, social media is the clear leader," said the report, which analyzed more than a trillion emails during the second quarter of this year.

Agari uses that analysis to create a Trust Index for email from the financial services, e-commerce, social media, travel, logistics and gaming industries.

The index is based on a Trust Score—a reflection of the adoption and deployment of security measures in an industry to protect its customers from malicious email—and a Threat Score, which provides a measure of relative risk based on malicious activity and attempted attacks.

Social media led all industry sectors during the second quarter with a Trust Score of 73 out of a possible 100.

Ranking companies and industries based on the Threat Score and Trust Score benchmarks gives consumers and leading brands insight into how aggressively a sector is being threatened and which companies are taking action to secure email and protect consumer data and trust, the report explained.

"Social media has been far more aggressive about protecting their customers and far more responsive to keep up with the technologies available to protect their customers," Agari founder and CEO Patrick Peterson says.

Among those technologies is domain-based message authentication, reporting and conformance (DMARC), which Agari's report says can virtually eliminate brand abuse through fraudulent email attacks and drastically reduces the risks of consumer loss, reputation damage and financial liability.

"A lot more people should be using DMARC because it allows administrators and organizations to be able to reject mail if it doesn't match certain parameters, no matter where it says it's coming from," says Paul Ferguson, vice president for threat intelligence at Internet Identity.

Nevertheless, Ferguson was skeptical of the glowing grades Agari gave social media. "We see daily campaigns with emails harboring malicious content that's masquerading as DHL, FedEx, Dun and Bradstreet, or social media like Facebook and LinkedIn," he says.

In fact, social media may contribute to the problem by fueling a growing culture of interrupting alerts that demand attention without forethought. "It allows bad guys to blend in with that noise," Ferguson says.

Other sectors analyzed by Agari didn't fare as well as social media. "The most significant, but not at all surprising, discovery comes from financial services, where there has been a huge spike in malicious activity, more than doubling from the prior quarter," the report said. "In fact, consumers are seven times more likely to

receive a malicious email from their bank than from any other type of company."

Despite that spike, financial services still managed a Trust Score of 40, a seven percent jump over the previous quarter and significantly higher than the worst sector in the report: travel, which scored 17.

"This sector, and the airlines in particular, is doing the least of all industries we analyzed to secure email and prevent their consumers from becoming

victims of an attack," the report said. "Even airlines like JetBlue that are well known for being leaders in delivering a better digital experience, are putting customers at risk with very little effort in preventing these types of attacks."

Agari also reported that many consumers do not realize that 95 percent of data breaches start with a phishing email. "I think we can safely say that after however many years it has been, we've lost the battle of educating about threats," says George Tubin, a senior security strategist with Trusteer. "We're just not going to be able to educate people to identify these things."

"We need to keep educating, but the only way we're going to be successful with this is to fight these technology attacks with technology defenses," Tubin says. "We shouldn't be relying on human judgement to determine what's a legitimate email and what isn't."

—John P. Mello Jr.





Car Hack Highlights March Toward Remote Control of Critical Systems

SECURITY RESEARCHERS WHO TOOK control of two popular vehicles by connecting a laptop to their internal computers moved a step closer to the day when people will be able to secretly commandeer a car from the driver, experts say.

By connecting cables to the cars' electronic control units, the researchers were able to use the software they developed to steer left and right, apply the brakes and move the fuel gauge to zero, the BBC reports. The test was performed on a 2010 Ford Escape and a Toyota Prius.

The vehicles' manufacturers did not consider the work a hack. That's because the

proof-of-concept, by Charlie Miller, a security engineer at Twitter, and Chris Valasek, director of security intelligence at IOActive, needed a wired connection, and the intruder had to be in the vehicle.

However, that logic misses the point, security experts say. Just because no one has been able to commandeer a vehicle by wirelessly hacking into its internal computers does not mean it won't happen eventually. Miller's and Valasek's experiment shows that experts are getting closer.

"What they're showing is every time they take a step, they're taking a new step forward," says Glenn Chisholm, vice president of

product management and CSO of Cylance.

In 2010, researchers from Rutgers University were able to wirelessly hack a car's tire-pressure monitoring systems and send a false low-pressure warning. The bogus signal was sent from a car traveling behind the target vehicle.

Of course, breaking into such a system is not nearly as complex as wirelessly hacking an ECU, which are cars' embedded systems that control steering, acceleration, braking and other critical functions.

Nevertheless, the 2010 experiment showed a wireless hack is possible, and the latest research demonstrates what could be done if an ECU were breached.

The fact that the Defense Department's Defense Advanced Research Projects Agency (DARPA) funded the latest work shows that the government believes that the growing number of computer systems in vehicles could present a safety threat.

"I believe that the digital attack surface for vehicles will undoubtedly increase in the coming years, and the fact that DARPA chose to sponsor Valasek's and Miller's work is a good indication that they see this field growing in importance," says Aaron Portnoy, vice president of research for Exodus Intelligence.

Car manufacturers insist they are paying close attention to security. Toyota told the BBC it has developed "very strict and effective firewall technology" against wireless attacks. Ford says the "safety, privacy and security of our customers is and always will be paramount."

Andrew Ginter, vice president of industrial security at Waterfall Security, says carmakers could learn from the nuclear power industry. There, monitoring systems are on one network while systems that control reactor operations are on a separate network that's closed to the outside. Ginter suggests the same architecture for vehicles, where separate computers are used for monitoring and for critical functions.

"If they're not connected, then the only thing you can hack over the network is the monitoring functions," Ginter says. "The safety-critical functions continue to work."

—Antone Gonsalves

CSO staff

risk

M E T R I C S G O V E R N A N C E C O M P L I A N C E A L L - H A Z A R D S



Forget Being CSO— Companies Need CROs

It's not enough to just build strong defenses. CSOs are now calculating risk profiles and may be looking at a title change as a result BY LAUREN GIBBONS PAUL

FEW WOULD DENY THAT THE CSO role has evolved quite a bit in recent years. At many large companies, the heads of both physical and information security now report to the same person, an enterprise CSO. The role is evolving as fast as the ever-changing threats it's designed to fight.

Many believe CSOs will morph, sooner rather than later, into chief risk officers (CROs), monitoring and mitigating enterprise risks, including those relating to information secu-

rity and facilities (but excluding financial risks, which are covered by the more traditional CRO function in large companies). At a high level, the new responsibilities include understanding your company's risk profile and risk appetite and then mitigating the risks accordingly.

Greg Thompson, VP of enterprise security services and deputy CISO at Toronto's Scotia Bank, already sees his role evolving into something like head of operational risk management. Scotia is Canada's third-largest bank.

"The writing is on the wall," says Thompson. "Ten years ago, this role was highly operational. We had to get better at operationalizing vulnerability management and putting the right controls in place."

As a CISO in heavily regulated industry in a risk-averse country, Thompson says he faces ever-greater reporting requirements and more need for expertise in operational risk management. He now tracks and manages the full gamut of non-financial risks: fraud, hackers,

hacktivists, breaches of privacy, configuration risk, risk of attack by nation states, reputational risk, facilities risk, IT process risk, compliance risk, and supplier and service risk.

"We used to just look at these as security risk indicators. Now, they are key risk indicators. We now look beyond information security and try to understand the rest of the picture," he says, adding that the regulatory climate is driving some of this new emphasis.

The New Metrics

Thompson is excited at the prospect of his role expanding, but he feels there is a lack of appropriate metrics to help him define and track enterprise risks.

"We need to find a set of metrics that speak to risk in real terms. There are things like mean time to patch, how many open audit findings. But that's not enough. Defining the measurements is the ultimate challenge," he says.

Right now, his organization is working on developing baselines that will be trustworthy markers now and in the future.

Relevant metrics are changing right along with the CSO role. For example, the information security function at Scotia Bank used to use "age of vulnerability" as an indicator of the level of risk under the assumption that the longest-standing vulnerabilities were riskier than new ones. Now, the bank focuses not on the age of the vulnerability but on the threat agents that exist to exploit the vulnerability.

Thompson believes that whether or not one's title includes the "R," every CSO takes

what he calls a "risk-related perspective" today, out of necessity. Verisign CSO Danny McPherson agrees, describing his approach as "intelligence-driven security," meaning he considers the context in which Verisign operates. "We want to use our best resources to make sure our high-value assets are protected," he says.

McPherson thinks enterprise risk management should be a cross-functional phenomenon.

"You need to break down those information silos. It's about connecting the dots for the business. How does a new product, a new press release, a new competitor—how do these affect the company's threat level, and how do we get back to an acceptable level of risk?" he says. "Given the global nature of business today, it becomes harder and harder to wrap your arms around that. How do we invest intelligently? How do we protect ourselves and our customers in the most effective way? Risk management needs to go beyond just checking off boxes that are required by regulations."

The only way you can protect the enterprise, McPherson believes, is by understanding the context and the landscape in which your business operates.

"If you can leverage that information and collect it and provide context, you will be more agile and adaptive as a result of that. And risk level goes down."

Scotia Bank's Thompson says information security now touches every aspect of business. And he's pleased to be helping his company manage the full range of risks it faces today.

It's no surprise that CSOs who already have a strong connection to the business are already well positioned to embrace the CRO role. Thompson and McPherson are both in constant contact with their business counterparts and enjoy that aspect of their jobs.

"I love getting a handle on the business context and contributing to the strategic direction," says McPherson. "It is so critical to have those feedback loops, to sit down together and challenge each other's assumptions." And he feels is lucky to have executive team support to do so.

"I couldn't do it without that."

■ Lauren Paul is a freelance writer and regular contributor to CSO.

Rise in Data Breaches Drives Interest in Cyber Insurance

GROWING AWARENESS of cyber threats and reporting requirements are driving a newfound interest in insurance policies that cover data breaches and other computing risks.

Almost a third of companies (31 percent) already have cyber insurance policies, and more than half (57 percent) of those that don't have policies say they plan to buy one in the future, a recent study by the Ponemon Institute and Experian Data Breach Resolution found.

"It's an issue that's much more front-and-center with senior executives in companies now," says Larry Ponemon, founder and chairman of the Ponemon Institute.

—John P. Mello Jr.

"The writing is on the wall. Ten years ago this role was highly operational."

—GREG THOMPSON, VP OF ENTERPRISE SECURITY AND DEPUTY CISO, TORONTO'S SCOTIA BANK



Small businesses—especially those vulnerable to natural disasters, like Japan's 2011 earthquake and tsunami, whose aftermath is pictured here—may find disaster recovery as a service particularly appealing.

3 Things to Consider Before Buying Into Disaster Recovery as a Service

DISASTER RECOVERY AS A SERVICE (DRaaS) backs up the whole environment, not just the data.

"Most of the providers I spoke with also offer a cloud-based environment to spin up the applications and data," which allows enterprises to keep applications available, says Karyn Price, a cloud computing analyst for consultancy Frost and Sullivan.

Vendors offer DRaaS to increase their market share and revenue. Enterprises, especially small businesses, are interested in DRaaS because it's inexpensive yet comprehensive. But before buying into DRaaS, a smart busi-

ness will first weigh the less-obvious factors, including these three.

1 Market drivers, vendors and differentiation

DRaaS is a smart move for cloud vendors hungry for a bigger slice of the infrastructure market.

"DRaaS is the first cloud service to offer value for an entire production infrastructure, all the servers and all the storage," says John Morency, a research vice president at Gartner. This opens up more of the market, providing much higher revenues for vendors.

DRaaS creates new revenue streams and opportunities for vendors, too.

"They want to bring comprehensive recovery to a wider variety of business customers," Price says. Where only an enterprise could afford a full-blown business-continuity and disaster-recovery solution before, now the cloud offers a more affordable option for small businesses.

Vendors offering DRaaS include Verizon TerreMark, Microsoft and Symantec (a joint offering), IBM, Sungard and NTT Data, Earthlink, Windstream, Bluelock, Virtustream, Verastream, EVault, Hosting.com and a trove

of smaller contenders seeking to differentiate themselves in the marketplace, according to Price and Morency.

"While most of the DRaaS vendors are relatively similar in their cost structures and recovery-time objectives, the recovery point objective is a differentiator between vendor offerings," says Price. Dell and Virtustream each report recovery point objectives of 5 minutes, but Windstream's range from 15 minutes to an hour, depending on the service, Price says.

2 DRaaS: No drab solution
DRaaS will probably continue to gain popularity. Companies looking to enter the cloud for the first time, those seeking a complete disaster-recovery solution or those that have infrastructure in severe-weather-risk locations are interested in DRaaS, but it's most appealing to enterprises with minimal tolerance for downtime.

"Most of the DRaaS vendors I speak with offer recovery times of four hours or fewer," says Price.

As for those that want to test the cloud for the first time, "If you are in the middle of a disaster and suddenly you have no infrastructure to restore to, would you rather have a cloud-based solution that maybe you would have been wary of as your primary option or would you rather have nothing?" asks Price.

The relatively low cost of a more comprehensive recovery solution is a big draw for small businesses. "DRaaS can minimize or even completely eliminate the requirement for company capital in order to implement a [disaster-recovery] solution," says Jerry Irvine, CIO of Prescient Solutions and member of the National Cyber Security Task Force.

Since DRaaS is a cloud solution, businesses can order it at almost any capacity, making it a more cost-effective fit for smaller production environments. Of the 8,000 DRaaS production instances that Gartner estimates exist today, 85 to 90 percent are smaller instances of three to six production applications, Morency says. These companies typically use between five and 60 virtual machines, and the associated production

storage is no more than two to five terabytes, Morency says.

The potential for bad weather also makes DRaaS appealing. "When you look at the aftermath of events like the tsunami in Japan, there is a lot more awareness and a lot more pressure from the board level to do disaster recovery," says Morency. This pressure and the affordability of DRaaS can tip the scales for many a small business.

failover core systems and not backup.

"Many organizations define their backup systems or data repositories as critical solutions for the [disaster-recovery] facilities to replicate," says Irvine. This provides for replication of core systems and data backup.

After the enterprise's data successfully fails over to the DRaaS service, at some point it has to be rolled back over to the enterprise infrastructure.

"When you look at the aftermath of events like the tsunami in Japan, there is a lot more awareness and a lot more pressure from the board level to do disaster recovery."

—JOHN MORENCY, RESEARCH VICE PRESIDENT, GARTNER

3 Proceed with caution
Enterprises and small businesses considering DRaaS must tackle a lot of due diligence before choosing a solution and face a lot of work afterwards.

"It's not like you just upload all the work to the service provider," says Richard Tracy, CSO of Telos. If a company is only allowed to copy data to a cloud under the condition that the cloud is supported by SAS70 data centers, then the DRaaS provider better be able to prove it has those data centers and agree to keep the company's data only in those facilities.

Depending on the industry, a customer may need to confirm that the DRaaS provider meets operational standards for HIPAA, the Gramm-Leach-Bliley Act, PCI-DSS, or some of the ISO standards.

"You don't want to trust that they do just because it says so on their website," says Tracy.

DRaaS can offer innate data replication and redundancy for reliable backup and recovery, but unless both services are specifically included, it may only include replication to

"You have to make sure that the DRaaS service will support you in that process," says Tracy. There are processes, procedures and metrics related to exit strategies for outsourcing that the customer must define during the disaster recovery planning process. These will depend on the organization. These procedures set the timing for how soon data restoration to the primary location takes place and how soon the company switches the systems back on.

"The [service-level agreement] should define the DRaaS provider's role in that," says Tracy. "It's not just failover, it's recovery."

The Upsides

DRaaS can replicate infrastructure, applications and data to the cloud to enable full environmental recovery. The price is right and the solution is comprehensive. Still in its early stages, DRaaS is by all signs worth consideration, especially with the number and types of offerings available and the obvious market need.

—David Geer

Workers Expose Data in Quest for Productivity

DO YOU KNOW WHICH EMPLOYEES could be the weak links in your organization? You might be surprised by the results of a recent study that asked participants to choose between protecting confidential information and getting work done

Imagine this: It's the day before an important presentation at a large corporation's annual global earnings conference. At the airport, the national sales manager receives last-minute feedback and is beginning to edit the document on a laptop when a stranger takes the next seat. The presentation, which contains proprietary information on important company financials, is now in plain sight of wandering eyes. The national sales manager is faced with a critical decision: continue working to finish the changes or stop altogether to safeguard the company data.

While every CSO would hope the employee would choose to protect the confidential information, the reality is that many would not. So how do you identify the weak links in the organization and prevent cybercriminals from gaining enterprise data through spear phishing and other low-tech methods like snooping?

The Ponemon Institute explored this topic in its "Visual Privacy Productivity Study." Employees at five companies were asked to participate in a survey. After being set up at a computer, the employees were told the survey would be delayed for 30 minutes and they had the choice to get some work done or take a break. Half of the employees' computers also had a privacy filter installed to determine whether visual privacy protection helped increase productivity. The study did find that employees whose visual security was protected with a privacy filter were twice as productive as those without a privacy filter. However, some potential weak links were revealed among those whose computers did not have a shield.

Millennials Choose Productivity

The study found a stark difference in privacy habits between generations, with older employees stating that privacy is either important or very important more often than their younger colleagues (65 percent of employees over 55 compared to 52 percent of those 26-35). These beliefs translated into outputs: Older employees that didn't feel the data on their screen was adequately protected worked

less than younger employees experiencing the same level of privacy. In general, with or without privacy, younger employees spent more time on the clock and were more productive.

Millennials are more likely to be privacy-complacent, choosing productivity over data security. This is a group that grew up with technology in hand; they aren't afraid of it and rely on it to get through the day. Tangible data, such as a manila folder containing papers with numbers and figures, is a foreign concept, making it easier for Millennials to access a file remotely without thinking twice about taking steps to secure it. Younger employees also feel pressure to produce more and prove themselves in a tight job market, leading them to cut corners on data security in favor of productivity.

Supervisors Choose Productivity

In general, the study found that those at or above the supervisory level are more productive than rank-and-file employees. The senior staffers with a privacy filter worked an average of 5.2 minutes, while those at a lower level without a filter worked an average of 1.8 minutes. However, senior staffers also worked longer when their data was not protected.

Supervisors likely face more pressure to be productive, but they also likely have access to more sensitive data, making them a risk area for a data leak.

Women Choose Privacy

Female employees worked longer and harder than their male counterparts and tended to be more conscientious about data protection. Fifty-six percent of all respondents said privacy was either important or very important, but 61 percent of women put a high value on privacy, compared to 50 percent of men. Gender also made a difference in time on or off the clock—when given the chance to work or walk away, women chose to work 62 percent of the time versus men's 48 percent.

—Larry Ponemon



CSO's e-Mail Newsletters

Keep Up To Speed On the Security Issues Important to You Delivered right to your desktop



CSO Update

A look at the latest security news and analysis on CSOonline.com, delivered three times a week.



CSO Salted Hash

IT security news and analysis, over easy, delivered daily.



CSO News Watch

A recap of the week's top news stories.



CSO Career

A twice-monthly newsletter of career and leadership-oriented news, articles and events plus job postings.



CSO Tech Watch

Twice-monthly update on technologies for protecting networks, facilities, employees, intellectual property and more.



CSO Security Leader

Biweekly leadership-related articles and reports from CSO, as well as tips for educating employees and corporate leadership.



CSO Continuity & Recovery

A twice-monthly review of published material concerning business continuity and disaster recovery.



Security Research & Metrics

A monthly roundup of useful security research, benchmarks and statistics.



CSO Risk Management

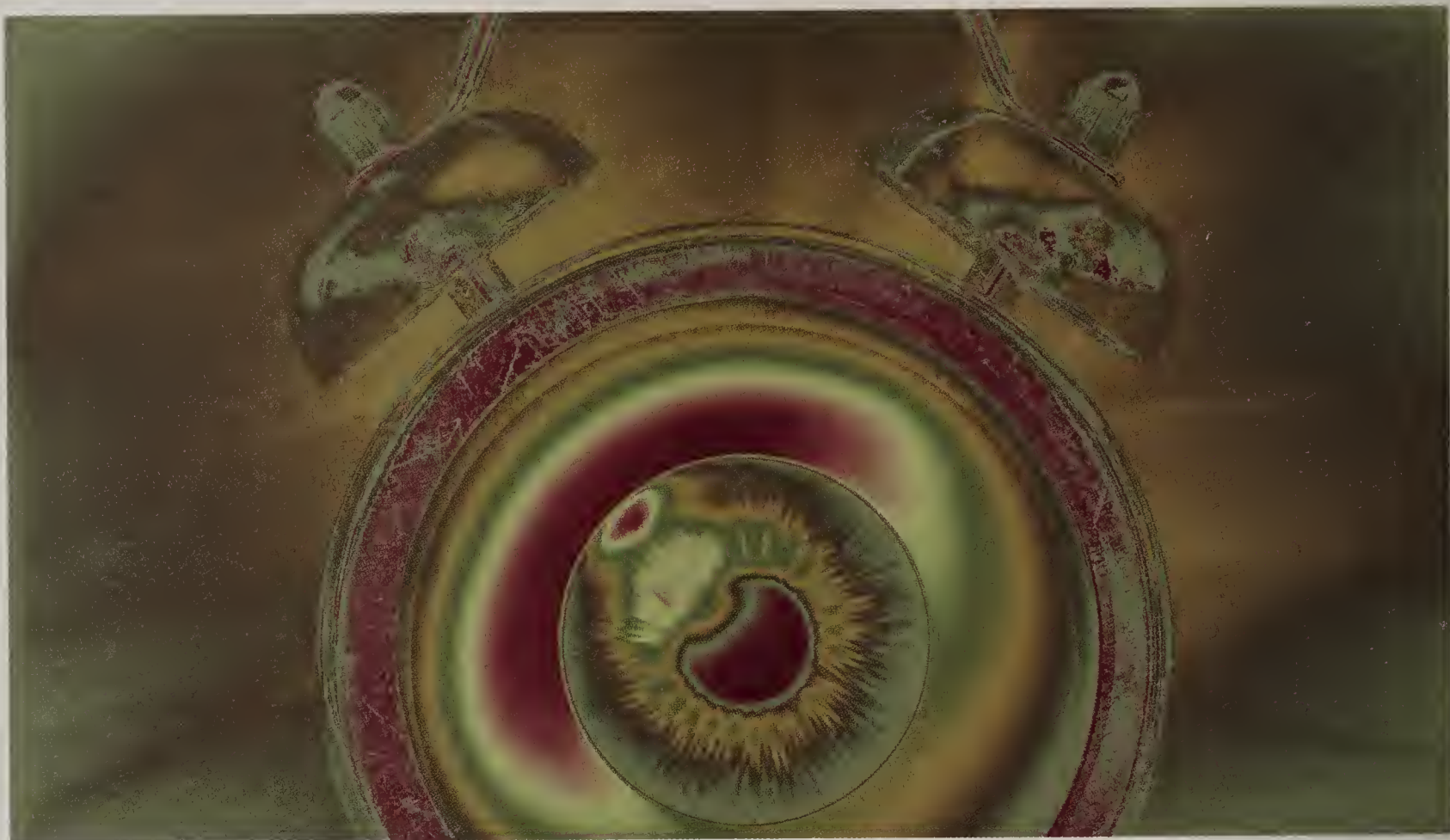
A monthly roundup of strategies and tools for accurate measurement and prioritization of risks.

Sign up now for CSO's
complimentary e-mail newsletters
www.CSOonline.com/newsletters

CSO
BUSINESS RISK LEADERSHIP

Lead

LEADERSHIP STRATEGY MANAGEMENT SKILLS CAREER



What Makes an Awareness Program Work

If you need help keeping your company's employees on the ball, check out these 7 tips for fixing your security awareness program BY IRA WINKLER AND SAMANTHA MANKE

WHEN WE WERE ASKED TO give the keynote presentation at a recent *CSO* event, we were pleasantly surprised to find that the top concern of the CSOs was security culture.

Thanks to performing many security assessments and penetration tests, we are keenly aware

that even the best technical security efforts will fail if the company has a weak security culture. It's heartwarming that CSOs are now moving past straight technological solutions and moving toward building a strong security culture as well.

To determine what makes a

truly successful security awareness program, we performed a study to identify critical factors that effective programs have in common. We interviewed security awareness practitioners at Fortune 500 companies and surveyed the security staff and general employees at the companies.

Additionally, we validated the results and gathered additional information at a security executive event in the United Kingdom with more than 150 security executives participating.

While there are many more lessons to be learned, what follows are the 7 most notable habits we

found that lead to successful security awareness programs.

1 C-level support.

Awareness programs that get C-level support are more successful. This support leads to more freedom, larger budgets and support from other departments. Anyone responsible for running a security awareness program should try to build strong support before focusing on anything else.

Yes, gaining this level of support can be difficult, but those who succeeded in getting it frequently did so by highlighting that security awareness was required for compliance and that awareness efforts provide an ROI and save the company money. They also created special materials specifically for upper management, such as newsletters and short articles that highlighted relevant news and tips that were specific to executives.

2 Partnering with key departments.

Successful awareness programs found a way to involve other departments, such as legal, compliance, human resources, marketing, privacy and physical security. While it is easier to do this if you have C-level support, these departments frequently have mutual interests and might be amenable to providing additional resources, such as funding or distribution, even without encouragement from above. Frequently, these departments also have the power to make security awareness efforts mandatory. For example, the legal and compliance departments can make security awareness a required

component of other processes, such as new-hire training.

To build this support, you might have to incorporate the needs of the cooperating departments into your general security awareness efforts. For example, you might suggest that you can use a security newsletter to include compliance content. If it gets you the support you need, the effort is definitely worth the trouble.

3 Creativity. Being creative is a must. A large budget helps, but companies with a small security awareness budget have still been able to establish successful programs through creativity and enthusiasm. For example, one creative security department used what it calls a "security cube" during a company event. In the main hallway, the department set up a mock cubicle that displayed 10 common security violations. Employees who could identify all 10 were entered in a prize drawing. Another effort included giving out boxes of chocolate that contained the security policy document on Valentine's Day. Employees reported that they felt compelled to read the document because they liked the chocolate.

4 Metrics. You can't claim to have built a successful program unless you have a way to prove it. The only way to do this is to collect metrics before you start the new awareness efforts. Without having a baseline, it is hard to demonstrate that your efforts were effective.

You could collect these metrics by distributing attitude surveys, by using a simulated phish-

ing attack to show how people respond before and after awareness training, or by documenting the number of policy violations, such as attempts to visit banned websites. When you can show measurable improvements in any aspect of security, you can justify your program and obtain additional funding and support. Just about every department in a company has to prove their value, and security should not expect to be an exception.

5 Being the department of how. Awareness efforts that focus on how to accomplish things are more successful than those that focus on telling people what they should not be doing. Clearly some activities should not be allowed, but those should be the exceptions and not the rule. For example, it is not realistic to ban employees from social networks and expect them to comply, but it would be useful to tell them how they can use social networks safely.

6 90-day plans. Most security awareness programs follow a one-year plan, often attempting to cover one topic a month. This is ineffective, as it doesn't reinforce knowledge or allow for adjustments based on feedback or new developments. Programs that rely on 90-day plans, reevaluating the program and its goals after each 90-day cycle, are more effective. The most successful program focuses on 3 topics simultaneously that are reinforced regularly throughout the 90 days. Every at the end of the cycle, the program is reevaluated to determine what should be addressed next.

7 Multimodal awareness materials.

The most successful programs are not only creative, but they also incorporate many types of awareness materials. While there may be a place for learning-management-system training modules, too many programs rely on them completely.

To keep employees interested, it's better to use many sources, including newsletters, posters, games, news feeds, blogs, phishing simulations, and so on. The most participative efforts appear to have the most success.

Be sure to include training materials that are likely to appeal to various demographics. For example, some videos may be targeted at young men, in which case you need to make sure that other videos or materials are aimed at older employees or women. There's no such thing as one-size-fits-all security awareness.

Conclusions

Of course these seven tips alone can't guarantee that your security-awareness program will succeed, but they're a good place to start. The big takeaway is that habits drive culture, and there are no technologies that will ever make up for poor security culture. Awareness programs, when properly executed, instills knowledge that guides behavior.

Security should be common sense, but you can't have common sense without common knowledge.

■ **Ira Winkler and Samantha Manke** are co-founders of **Secure Mentem**, a consultancy focused on security-awareness services.



Beef Up Defenses Without Breaking the Bank

TODAY'S SECURITY THREATS SPAN A broad spectrum of social engineering schemes, international hackers, and insider threats. It's hard to know how to keep up, let alone stay ahead of the curve.

"Security functions are getting only 70 percent of the resources that they need to do an adequate job," says Michael Versace, insights director of worldwide risk at IDC. "The hard stuff is in the next 30 percent."

Meanwhile, worldwide spending on security infrastructure, including software, services and network security appliances used to secure the enterprise, rose to \$60 billion in 2012, up 8.4 percent from \$55 billion in 2011, according to Gartner. That number is expected to hit \$86 billion by 2016.

Security experts offer five tips for enhancing security that don't cost a lot of cash—some are even free—so companies can spend their security dollars on the hard stuff.

1 Patch security holes and identify vulnerabilities. Three of the top 10 botnets reported in February 2013 were more than 8 years old, according to FortiGuard

Labs, the threat-researching arm of network security firm Fortinet. In the most successful attacks, most of the exploits had been identified and fixed by vendors years earlier, says Derek Manky, global security strategist. Companies need to keep patches up-to-date.

"We see this time and time again," Manky says. "There are always software security flaws that hackers go after, and that's how they get into systems—through attachments or a link to a website that got somebody infected. That usually happens through [tools] like Firefox, Internet Explorer, Java, Flash, Adobe Reader and Mozilla. So apply your patches, at least to these top targets."

For more advanced security, inexpensive vulnerability identification software will probe your systems looking for security holes and will help identify solutions.

2 Install your free firewall and antivirus upgrades. A lot of people don't realize their basic support contracts with most vendors for support, firewalls and antivirus include free upgrades, says Andy Hubbard, senior security consultant at Neo-

hapsis, a security services firm.

"If you don't have a strategy to revisit what the available technology is that you've already paid for, then you're missing out on a lot of new features and enhancements," Hubbard says. "It only takes your effort to do the research. Call your vendor and revisit your firewall and antivirus solution contracts."

3 Keep up with BYOD. Personal devices in the business environment are here to stay. Yet 79 percent of businesses had a mobile security incident in the past year, including malicious apps downloaded to a mobile device, unsecured Wi-Fi connections and lack of security patches from services providers, according to a mobile security report by Check Point Software Technologies. These incidents cost companies between \$100,000 and \$500,000 in staff time, legal fees and resolution processes.

Organizations can improve mobile device security by using bring-your-own-device (BYOD) policies or user agreements to ensure workers take security precautions. The checklist should include installing available

upgrades and patches, ensuring that each mobile device infrastructure component has its clock synced to a common time source, and reconfiguring access-control features as needed, according to the computer security division of the National Institute of Standards and Technology.

Information security teams should also periodically perform assessments to confirm that their mobile device policies, processes and procedures are being followed properly. Assessment activities may be passive, like reviewing logs, or active, like performing vulnerability scans and penetration testing.

4 Define a firm-wide security strategy. Nine out of 10 big companies lack defined security plans, or the plans aren't tied to business goals and business objectives, says Kristine Briggs, vice president of corporate operations at Neohapsis. "There's no way to know if you're supporting business objectives unless you take the time to develop the security strategy and make sure they're doing the most important things for overall risk reduction," she says.

"Some of what we found would shock most people," says Briggs. "We even find that in entirely regulated industries." At one "very large" and highly regulated company, a critical platform was supporting the majority of revenue for one of its internal customers, yet it didn't have a defined security strategy or plan.

"Although they had massive goals for revenue growth for the use of that platform, they weren't taking into account the end customer's compliance requirements, but customers assumed they had this covered," Briggs says. "They had no plan to map to the technology infrastructure or to the business growth that's planned. That could bite them very easily" if the platform is breached or crashes.

The strategy and plan don't require outside expenses, and when complete will reduce the overall cost of running the environment "because you're doing

things in a planned and repetitive way that improves security and reduces risk. If you get the right people in the room for a half-day session, you should have it 80 percent done, she says. Those people should represent both business and technology, and any other stakeholders.

"Most people do a one-year plan, and should answer the questions: What are the company's business objectives? What risks are associated with those objectives? For instance, is the business highly regulated, or do they perform financial transactions? What type of data resides in the IT environment? What technologies are already available to protect the data? And what does the budget allow for new technologies?"

5 Educate employees. Successful attacks usually exploit the human mind. "Humans are always the weakest link in the chain," Manky says.

Education can help stop employees from falling victim to phishing attacks, social-engineering schemes, or careless use of their login credentials, which accounted for three of the top 10 attacks against large companies, according to Verizon's 2012 "Data Breach Investigations Report."

But the stereotypical wall posters with security tips hanging in the break room are useless, says Julie Peeler, foundation director at (ISC)², a global nonprofit that educates and certifies information security professionals.

"Security training is not a one-time event. It has to be integrated throughout the entire organization, and it has to come from the top," she says.

When it comes to security, managers need to ensure that employees understand the security posture of the company from day one, Peeler says. They must be willing to sign confidentiality agreements, attend training and participate in ongoing awareness, all with the goal of remaining vigilant.

—Stacy Collett

SOCIAL SECURITY

INDUSTRY CHATTER ON TWITTER

"Clicco ergo sum" seems to sum up the world of online interactions, both malicious and benign, pretty well.

—Lenny Zeltser @lennyzeltser

Must remember that loud sounds on roof are from roofer and not falling tree or one of @attritionorg's minions.

—Security Humor
@SecurityHumor

"Neighborhood safety warning (Sex Offender activity in your area)"—phishing ...Clever. I'm still not clicking.

—Rafat Łoś @Wh1t3Rabbit

Your task, should you choose to accept it, is to come up with a compliance initialism for "WTF."
#WhatStandards

—Martin McKeay @mckeay

Using IT Skills to Help the World's Poorest

BACK IN 2007, JOHNNY LONG CAME to a fork in the road. An accomplished IT security pro who had spent 13 years working at a big-name company, he had a great career and family, but he didn't feel fulfilled. And he had no idea why not.

The wheels began to turn when his wife came home from a Christian mission in Uganda later that year. She showed him video and pictures she had taken of African children, many of them orphans, laughing and dancing despite their extreme poverty.

"I had done everything there was to do in my career, but I was still miserable," says Long. "I had to figure out what those kids had that I didn't."

For a year or so, Long made regular two-week trips to work in Uganda but continued at his job at CSC in Virginia. He soon found that wasn't enough. So he and his wife made a huge commitment: They sold their house, quit their jobs and moved the kids to Uganda, offering help sorting out computer problems.

As Long soon discovered, computer viruses and security holes were the most pressing problem he would encounter. Thankfully for local residents, Long's skills matched beautifully with their needs.

Now, he is head of a charitable organization he founded, Hackers for Charity, which pairs up people who have IT security and other tech skills with charitable groups that need help.

To Long, it quickly became apparent that the Ugandans he encountered needed a lot of help with technology.

"They live in mud huts. I didn't even think about computers being there," he says. But as it turns out, computers and smartphones are crucial for both locals and charitable organizations operating in Africa.

"The nonprofits have to keep in touch with the U.S. and Europe because that's where their donors are," says Long. Any loss of connectivity—which was an everyday occurrence in his area—meant their fragile links to sources



Johnny Long, founder of the nonprofit Hackers for Charity, was inspired to start his foundation after his wife returned from a trip to Uganda

es of funding and jobs were in jeopardy.

"They don't know where the money is, they don't know if they can feed kids. They don't know if money has been wired, they can't sponsor a new kid. That's where this whole thing started," he says.

"Computer viruses are rampant in Africa," says Long, as is pirated software. "It has to do with the mentality of growing up in a village. If your neighbor has extra corn flour, they share it with you. Sharing is the culture. It's part of who they are."

When it comes to technology, the attitude is the same, he says. Pirated software is sharing. People often share applications and files on infected flash drives.

"We see tons of machines that are obliterated because of viruses," says Long.

Long also helps detect and prevent cybercrimes such as identity fraud, insider and outsider threats. In addition to doing some consulting for the government and banks, he also teaches residents sought-after security skills like penetration testing.

"You have to teach them offensive skills and trust they will use them for good," says Long.

Sometimes it can be difficult to know who will stay on the side of the good guys. Be-

cause of the dire economic climate, people can come under pressure to use their new chops for personal financial gain. Long does not want to see that happen, so he chooses his students carefully.

Getting Hackers for Charity off the ground was not easy. In the early years, Long's family survived off a combination of donations from other computer people and Long's security consulting gigs, which he believes hurt his focus.

Now, the organization is 100 percent donor funded. And Long's conviction he is doing the right thing is solid.

"Inherently, we all understand what it means to be successful, though everyone has an idea of what success is. Fulfillment is different. You don't always see that in the workplace. Fulfillment comes when you step out and use your skills to help someone do something they could not do any other way," he says.

Long's group is constantly looking for more security professionals to volunteer.

"You don't have to go to Uganda to get connected. There is stuff right in your neighborhood that needs doing. Often, you don't even have to leave your keyboard," he says.

—Lauren Gibbons Paul



CSO
40
AWARDS
2014

Call for Entries



SECURITY MEANS BUSINESS

The best security projects create opportunities for business growth—entering new markets, operating more efficiently, prioritizing resources and fostering organizational agility.



In its second year, the **CSO40 Awards** will recognize 40 security initiatives for outstanding business contributions. Whether it's a new system, new processes, or a novel organizational approach, we want to know about your best work, and how you measured its value to the enterprise.

APPLY

Nominations will be judged by a panel of veteran security leaders and industry experts, working together with CSO's editors.

APPLY TODAY AT WWW.CSOCONFAB.COM/2014AWARDS

ATTEND

CSO40 Award honorees will be recognized at the CSO40 Security Confab + Awards event, March 31-April 2, 2014 at the Chateau Elan Resort outside Atlanta, GA. This event is security leaders' best forum for networking and exchanging ideas that work.



DON'T BE LATE!

THE DEADLINE FOR NOMINATIONS
IS SEPTEMBER 16, 2013!

PRODUCED BY
CSO

WHAT KIND OF TARGET ARE YOU?

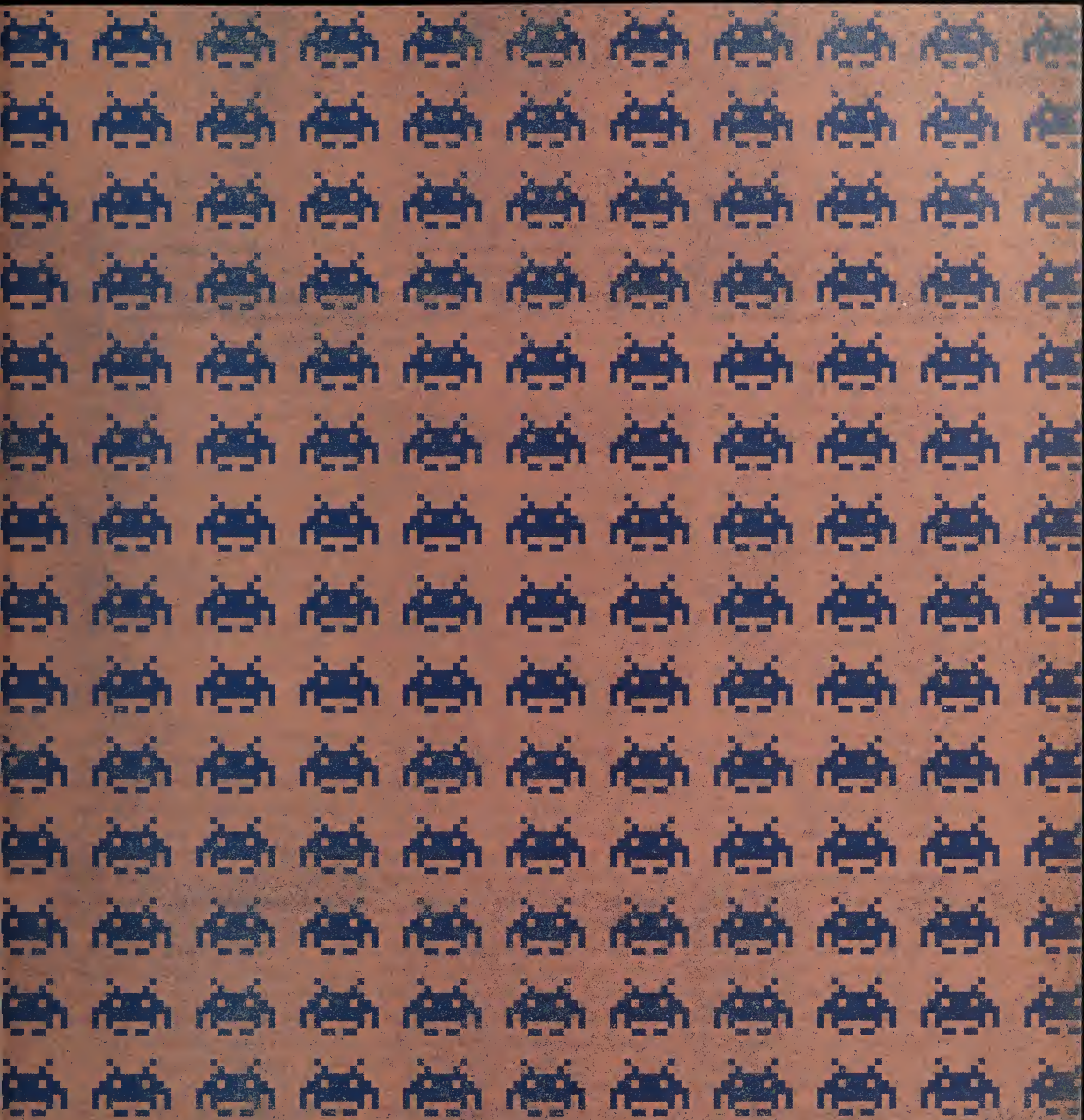
Some attackers want money or data, while others hope to make you look bad. What do you have that might put you on a hacker's hit list?

BY BOB VIOLINO

Is your organization a likely target for security attacks? While any company can be victimized by breaches, some enterprises have a much greater chance than others of being on the hit list, according to security experts and executives.

One of the most common ways organizations expose themselves to attacks is by giving cybercriminals a chance to break through. The majority of those that suffer attacks are targets of opportunity—not specifically chosen but attacked because they exhibited a weakness someone knew how to exploit, according to the “2013 Data Breach Investigations Report” from Verizon Enterprise Solutions, a unit of Verizon Communications.

“An opportunistic attack happens because the attacker was



Cover Story

presented with an opportunity and said, 'Why not?'" says Wade Baker, managing principal of the Verizon Risk Team and principal author of the data breach report.

More often than not in these cases, the organizations had something connected to the Internet that shouldn't have been, Baker says. Certain services companies run online "are like a beacon that says 'attack me,'" he says. "Cybercriminals are constantly running scans looking for known vulnerabilities such as FTP, and if you're running FTP and expose that on the Internet, it's almost certain that you will have attacks aimed your way."

Organizations that do an extremely poor job taking care of the basics, such as operating system and device patching and configuration and secure application coding, are far more likely to fall victim to opportunistic attackers who are looking for the easy targets, says Bob Rudis, director of enterprise information security and IT risk management at Liberty Mutual Insurance.

"It's far too easy to do a basic vulnerability scan or even just perform look-ups in SHODAN [a search engine] to hunt for potential victims," Rudis says. "It's almost a guarantee that if you have something that is Internet-facing and haven't done the bare-minimum basics, you're going to have those assets fall victim to a successful attack. Whether that results in a full-on breach or not is a variable that has many factors."

Three-quarters of breaches result from simple opportunistic attacks, not highly determined and sophisticated groups, according to the Verizon report. The study consists of data—covering more than 47,000 reported security incidents and 621 confirmed data breaches from the past year—gathered from 19 global organizations, including law-enforcement agencies, national incident-reporting entities, research

institutions and private security firms.

While the exact percentage of attacks that result from vulnerability scans is difficult to ascertain, Baker is fairly sure it's a large majority of all cyberattacks, possibly more than 90 percent. "This [scanning] goes on constantly," he says. Attackers are looking at point-



of-sale systems, certain types of remote desktop services, blogging platforms, and other systems that can have weaknesses.

"There are so many [vulnerabilities] out there, and there are different lists where people can find vulnerabilities," Baker says. "They show what actions and techniques different criminals use."

But online exposure isn't the only problem that makes companies targets for attack.

"Attackers look for vulnerabilities in both machines and people," says Phil Hochmuth, program manager of security products at research firm IDC, which is owned by CSO's parent company. "This is to say, they scan Web servers for vulnerabilities which could be exploited to gain access to sensitive data, [and] they also look at individuals working for target organizations and go after them with targeted attacks, with the goal of getting access via the

employee's credentials or identity."

The Verizon report notes that "all kinds of organizations—from government agencies to iconic consumer brands, Internet startups to trusted financial institutions—have reported major data breaches in the last year." But it also shows that certain characteristics make some companies more likely targets.

For example, 37 percent of breaches during the past year affected financial organizations (more than any other type of business); 24 percent of attacks occurred in retail environments and restaurants; and 20 percent of network intrusions involved manufacturing, transportation and utilities.

Although most attacks are opportunistic, according to the report, that's not to say all attackers lack motives when they select targets. Often organizations are singled out because they have something that's enticing to a hacker or other criminal, or are known to be vulnerable to particular types of attacks, Baker says.

"They are targeted because of the types of data they have," Baker says. "So for financially motivated crimes, if you process payments or credit cards, then you're a target. If it's online threats, then just by having an IP address, you're a target. If it's espionage, if you have intellectual property that people want, then that makes you more of a target."

Avivah Litan, vice president and distinguished analyst at research firm Gartner, agrees that many cybercriminals are going after specific types of data, and they're taking aim at specific types of technology tools companies use so that they can break in and achieve financial gain.

For example, online retailers might be a likely target of breaches because they use shopping carts or certain point-of-sale systems that are vulner-

able to security breaks. Cybercriminals "go out there and study which sites have the equipment they know" is vulnerable, Litan says. "They go where the money is," she says. "Any financial services company, a payments processor or a bank or a mutual fund firm [is vulnerable]. They're attacked all the time."

Rudis agrees that organizations that have fluid financial assets, such

down the power grid. Other likely targets include patent firms (for intellectual property) and healthcare organizations (for insurance scams).

In short, "if a company has something the bad guys want, it will be a target," Litan says. "I don't think criminals necessarily know who has lapsed security processes. But any company with lax processes is more vulnerable than ones that are better prepared."

"SMBs are increasingly being targeted, especially small e-commerce firms or financial organizations," Hochmuth says. "These companies often have a bad combination of circumstances: limited IT resources and security technology, combined with something [digital] worth stealing, usually customer payment data. Criminals have targeted these types of companies for years, especially as large

"If an organization has a large population on social media or they use social media in ways that attract the wrong kind of attention, they will definitely need to pay attention to that vector."

—BOB RUDIS, DIRECTOR OF ENTERPRISE INFORMATION SECURITY AND IT RISK MANAGEMENT, LIBERTY MUTUAL INSURANCE

as banks, are going to continue to be targets at both the technology level and the personnel level, "and by a cadre of different actors" including organized crime, activists and terrorists.

But there are plenty of other motives that drive bad guys to attack particular targets. "Organizations with valuable intellectual property—software, pharmaceutical, electronics, manufacturing—are likely targets, as they potentially have digital assets that could be valuable to a competitor," Hochmuth says.

High-tech companies, such as chip or disk-drive manufacturers, are also a huge target because of the product information they have, Litan says. Security companies are targets because criminals are looking for insights they can use to break into systems or exploit weaknesses in software. Organizations that either support controversial issues or get into the headlines for other reasons can become the targets of activists, Rudis says.

Utility companies might be a target for hackers who are looking to take

Indeed, the way companies use technology resources, such as social networking, can play a key role in opening them up to security breaches.

"If a major corporation doesn't think about how it uses social media at all and just blabs on about anything, it certainly can become a target," Baker says. "We've seen that, where companies engage in something that is viewed by a certain segment of the population as being out of step. Attacks have started because of that. Social media is a good way to be out there, but it can backfire."

Rudis agrees that social media, if used incorrectly, can make organizations targets for attack. "If an organization has a large population on social media or they use social media in ways that attract the wrong kind of attention, they will definitely need to pay attention to that vector," he says.

Attackers may also factor in the size of the organization when deciding who to target. Small and midsize businesses (SMBs) might be particularly vulnerable because they lack resources and sophisticated security programs.

enterprises have begun investing more in information security."

It's not necessarily a matter of attackers specifically looking for smaller businesses to attack. But in scanning for vulnerabilities, they're liable to come across organizations that have left themselves open for attack—and often it's smaller companies that don't have the resources or the knowledge to lock themselves down, Baker says.

Franchises can also be at risk, because when hackers find a vulnerability that they can exploit against one franchisee, that same exploit often works on other franchisees as well.

Clearly, there are many factors that can make organizations targets for security attacks. Companies must be diligent about implementing the proper security mechanisms, and if necessary, revamping processes or the way they expose information and systems to minimize their risk.

■ Bob Violino is a freelance writer and editor. He can be reached at bviolino@optonline.net.

last



Ten Tweets David Litchfield

@dlitchfield

Database security expert David Litchfield gives us his perspective on database forensics, bad security movies and swimming with sharks in 140 characters or less

CSO: Let's start with your origins in the industry. How did you get started in security?

David Litchfield: I watched *The Net* with Sandra Bullock in '95 and was intrigued. I wanted to know more, so I switched from a zoology degree to a computer science degree.

So a Sandra Bullock movie inspired your career?

It did... Rewatching the film these days, I cringe at the technical errors.

Yes, that's definitely a movie that gets panned quite a bit by security folks! What led to the interest in database security?

My area was buffer overflows. In 2003, I wrote a paper on defeating GS and SafeSEH. After that, I needed a new challenge.

Interesting. What would you point to as one of the most major changes in security since you first started in the profession?

Probably Microsoft's improvement in security led by Trustworthy Computing and the Security Development Lifecycle.

And what excites you these days about being a security professional?

Database forensics. It's an area receiving very little attention, but it's so important after a breach.

What's your security philosophy? And how do you apply it to your daily work?

Minimize risk as best you can, but be vigilant and prepared for when your defenses are breached. I realized in 2007 that 100 percent software security is not going to happen any time soon, so I switched from bug hunting to forensics.

A bit of Internet research reveals you are also a photographer and you like to photograph sharks. Why? Tell us more!

I love nature, especially the sea, and it's my escape. It's very humbling to confront a great white and look into its eyes.

Wow. Humbling, indeed! I also read you were once a U.K. track-and-field star. Compare that with working in security.

Both require hard work and dedication. A posterior cruciate ligament injury ended my track-and-field career; security is sedentary.

Ha! Sedentary? Depends on the day, right? Complete this sentence: If I weren't working in security, I would _____.

If I weren't working in security, I would be working as a stunt double for Steve Backshall.

Cool! I do see a resemblance. Thanks, David; we've gone through 10 tweets. Who should CSO tweeterview next?

Try @PortSwigger or @arnimarhardar.

BIG DATA, BIG RISK.

Securing Big Data is a business imperative.

Big Data offers enormous business benefits - and an attractive target to cyber criminals. Protect What Matters.™

THE CLOUD

LOVES A WINNER.

With the cloud as your ally, we predict an unprecedented winning streak for your business. Because a smartly managed cloud means an unstoppable cloud. And in our experience, unstoppable tends to mean you win. bmc.com/thecloud



IT'S AMAZING WHAT I.T. WAS MEANT TO BE.